



# Fundamental Capabilities of Effective All-Hazards Infrastructure Protection, Resilience, and Emergency Management for State Departments of Transportation

September 2015  
**AVA** Documents  
Document Sharing Hub

© 2015 by the American Association of State Highway and Transportation Officials. All rights reserved.  
Duplication is a violation of applicable law.

Publ Code: HAZ-1      ISBN: 978-1-56051-638-5

© 2015 by the American Association of St  
All rights reserved. Duplication

Full document details: [AASHTO HAZ-1-2015](#)

# Foreword

In the days, months, and years following the events of September 11, AASHTO and its partners united through the Transportation Research Board to improve and enhance the skills of the transportation community to prepare for and respond to events of terrorism that threaten the transportation system. One of many products produced was a *Guide to Understanding the Fundamentals of Effective Security Management*. In the intervening years it has become clear that the learning achieved not only applied to security threats but to all forms of threats to the transportation system.

Today we understand that:

- **Customers today have higher expectations for system performance and reliability and lower tolerance for delays.** Even small events pose threats of great consequences since the impact of any incident is magnified.
- **Hazards continue to evolve. Extreme weather, cyber incidents, and other additional hazards need to be addressed.** In addition, the risk of natural and man-made events is growing more common due to many pressures, including an aging infrastructure.
- **Today's transportation systems are integrated cyber and physical systems.** There has been, and continues to be, significant deployment of new technologies to support DOT activities.

This newly updated Fundamentals Guide synthesizes the most recent federal and state guidance and research efforts from a state DOT perspective and lays out a set of capabilities for state DOTs that addresses all-hazards infrastructure protection, resilience, and emergency management and reflects National Preparedness Goals. The goal of the Guide is to provide a resource for state DOTs that supports the integration of infrastructure protection and resilience into all of their operations and infrastructure programs.

To ensure the security and resilience of our nation's transportation systems, AASHTO member DOTs, along with local, state, and federal emergency response agencies have become strong security and emergency response partners. This Fundamentals Guide provides you the best and latest thinking on how to remain the best at what we do and how we can remain that way moving further into the 21<sup>st</sup> Century. This Guide and our partnerships will help to keep the nation's transportation system strong and well protected no matter what the event that may threaten it.



John Cox  
Director  
Wyoming Department of Transportation  
2015 AASHTO President



Brian Ness  
Director  
Idaho Transportation Department  
Chair, AASHTO Special Committee on Transportation  
Security and Emergency Management



# Preface

This guide is an update to the 2007 *Fundamentals of Effective All Hazards Security Management for State DOTs*. The original guide was intended to provide DOT managers with an overview of an effective all-hazards security management program. It outlined the fundamental responsibilities of a state department of transportation (DOT):

1. Prevent incidents within their control and responsibility;
2. Protect transportation users, agency personnel, and critical infrastructure;
3. Support regional/state/local emergency responders with resources including facilities, equipment, and personnel;
4. Recover swiftly from incidents;
5. Evaluate response(s) and continually improve plans, training, skills, and protocols.

Since the time of that publication, the fundamental responsibilities of DOTs have not significantly changed but the capabilities necessary to perform those responsibilities have evolved. AASHTO has recognized five “fundamentals” documents, most published since 2009, that provide comprehensive guidance on the major elements of a state DOT all-hazards transportation security and emergency management program:

1. *Security 101: A Physical Security Primer for Transportation Agencies* (2009; update anticipated 2017)
2. *A Guide to Emergency Response Planning at State Transportation Agencies* (2010; update anticipated 2016)
3. *Blast Resistant Highway Bridges: Design and Detailing Guidelines* (2010)
4. *Costing Asset Protection: An All Hazards Guide for Transportation Agencies* (2009; update anticipated 2016)
5. *Continuity of Operations Planning (COOP) Guidelines for Transportation Agencies* (2005)

Since 2010, four significant national-level directives and executive orders have been issued:

- **Presidential Policy Directive 8: National Preparedness** (2011) strengthens security and resilience through five preparedness mission areas: prevention, protection, mitigation, response, and recovery.
- **Presidential Policy Directive 21: Critical Infrastructure Security and Resilience** (2013) focuses on the need for secure critical infrastructure that is able to withstand and rapidly recover from all hazards (resilient).
- **National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience** emphasizes the importance of resilience, and the need to reduce all-hazards vulnerabilities and mitigate potential consequences of incidents or events that do occur.
- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity** (2013) provides a technology-neutral cybersecurity framework and means to promote the adoption of cybersecurity practices.



# Table of Contents

|                                               |    |
|-----------------------------------------------|----|
| Foreword . . . . .                            | 1  |
| Preface . . . . .                             | 3  |
| Introduction . . . . .                        | 7  |
| Summary of Fundamental Capabilities . . . . . | 11 |
| Planning . . . . .                            | 13 |
| Public Information . . . . .                  | 17 |
| Operational Coordination . . . . .            | 21 |
| Prevention . . . . .                          | 25 |
| Protection . . . . .                          | 29 |
| Mitigation . . . . .                          | 33 |
| Response . . . . .                            | 37 |
| Recovery . . . . .                            | 41 |
| Cybersecurity . . . . .                       | 43 |
| Training and Exercises . . . . .              | 49 |
| Appendix A: Selected References . . . . .     | 51 |
| Appendix B: Definitions . . . . .             | 53 |
| Appendix C: Acronyms . . . . .                | 67 |



# Introduction

Evolving DOT priorities, research on security and emergency management, and new federal guidance issued since 2010 have prompted the need to re-examine DOT capabilities to support their fundamental roles. The 2007 version of the Fundamentals document focused on capabilities associated with security awareness, critical infrastructure/key asset protection, and readiness, response, and recovery. There is now an emerging focus on the complementary goals of infrastructure protection and resiliency as part of security and emergency management.

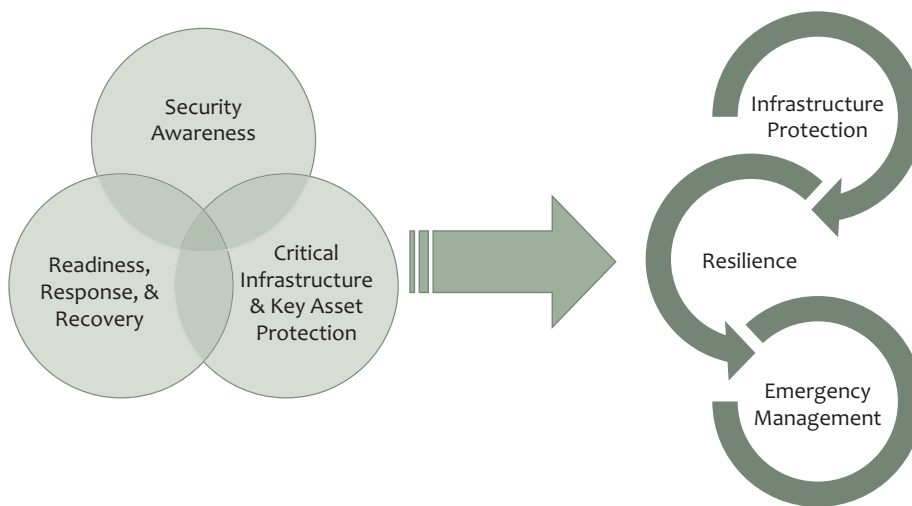


**Figure 1.** DOT Capabilities—2007 and Now

- **Customers today have higher expectations for system performance and reliability and lower tolerance for delays.** Even small events pose threats of great consequences since the impact of any incident is magnified when a transportation network is operating at or past its capacity—as is the case in portions of many states as travel demand on their transportation networks grows.
- **Hazards continue to evolve.** Extreme weather, cyber incidents, and other events need to be addressed. In addition, the risk of natural and man-made events is growing more common due to many pressures including aging infrastructure.
- **Today's transportation systems are integrated cyber and physical systems.** There has been, and continues to be, significant deployment of new technologies to support DOT activities.

DOTs have a significant role in infrastructure protection. Transportation employees and contractors are the best positioned to know what is usual and unusual and can help their agency protect its employees, information, data, networks, and facilities. DOTs have the responsibility for controlling access to critical components, establishing coordination with law enforcement to ensure quick response to incidents, conducting risk and vulnerability

### National Preparedness Goals

- Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
- Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
- Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts and by employing effective responses to save lives and ensure the rapid recovery of essential services;
- Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
- Promote learning and adaptation during and after exercises and incidents.

assessments, and taking action to mitigate the effects of those risks and vulnerabilities. In addition, transportation agencies have institutional heft—in terms of their broad policy responsibility, public accountability, large and distributed workforces, heavy equipment, communications infrastructure, and their ability to swiftly take direct action—that provides a stable base to systematically reduce risk to transportation infrastructure over time.

Resilience is “the ability to prepare and plan for, absorb, recover from and more successfully adapt to adverse events” (*Disaster Resilience: A National Imperative*, National Research Council, 2012). DOTs are currently in the process of understanding the impact of the shift in focus from protection of assets to resilience of systems. In the context of transportation and infrastructure, the principles of resilience are shown in the box at right.

Overall DOT efforts have improved emergency response planning and training since the 2007 version of this Fundamentals document. When an emergency occurs, routine day-to-day operations give way to a focused, practiced, and resilient crisis management approach that requires professional skills throughout the breadth and depth of the organization. Traffic Incident Management (TIM) provides processes and procedures for responders (firefighters, emergency medical services, law enforcement, towing and recovery, safety patrols, transportation and maintenance crews, and 911 professionals) to work together as a team to clear incidents safely and quickly. The National Incident Management System (NIMS) integrates best practices into a comprehensive framework for use by emergency management personnel at the local, state, and federal levels. The Incident Command System (ICS) provides the integration of facilities, equipment, personnel, procedures, and communications for emergencies.

### Resilience Principles

- Redesign to reduce or eliminate vulnerability.
- Improve ability to improvise during an event.
- Add redundancies to system to improve availability to reroute traffic through one or more parallel components.
- Have backup components available to quickly replace disrupted function.
- Allow rerouting.



This 2015 Fundamentals document synthesizes the recent federal and state guidance and research efforts from a state DOT perspective and lays out a set of capabilities for state DOTs that addresses all-hazards infrastructure protection, resilience, and emergency management and reflects national preparedness goals. The goal of this document is to provide a resource for state DOTs that supports the integration of infrastructure protection and resilience into their operations and infrastructure programs.



# Summary of Fundamental Capabilities

Figure 3 provides a summary of the fundamental capabilities necessary to support the DOT's responsibilities, organized by categories that mirror the National Preparedness Strategy:

- **Prevention:** To avoid, prevent, or stop a threatened or actual act of terrorism.
- **Protection:** To secure against acts of terrorism and man-made or natural disasters.
- **Mitigation:** To reduce loss of life and property by lessening the impact of disasters.
- **Response:** To save lives, protect property and the environment, and meet basic human needs after an incident has occurred.
- **Recovery:** To assist communities affected by an incident to recover effectively.

Fundamental capabilities of DOTs reflect an all-hazards approach including extreme weather, storm surges, natural events, accidental or unintended incidents, technological failure, and cybersecurity breach, and multi-modal risk assessment and management.

The capabilities reflect an all-hazards approach that includes a broad range of incidents and events that have potential to impact transportation systems operations. Extreme weather, cyber incidents, and other additional hazards need to be addressed as part of an all-hazards approach. Figure 2 includes the types and frequency of events that transportation agencies may encounter along with the other agencies (local, state, and federal) that may be involved depending on the severity or complexity of the incident.

The following sections provide a definition of each category, an overview of the key capabilities required for that category, and resources to support the implementation of those capabilities.

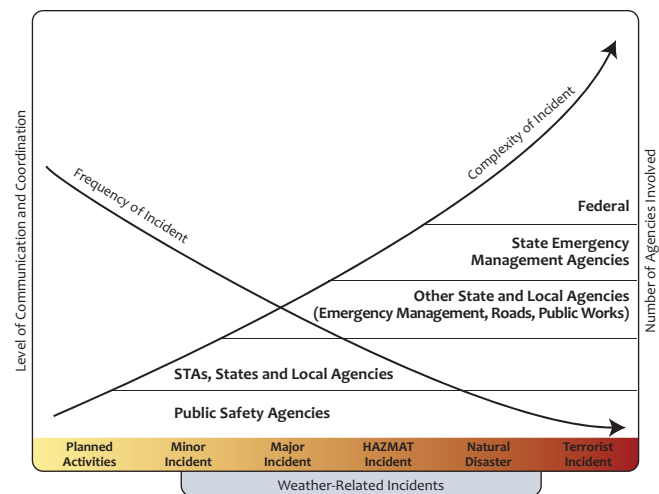


Figure 2. Agency Involvement by Incident Level

Source: NCHRP 525 Vol. 6, Security Guide for Emergency Transportation Operations

---

**Planning:** Conduct a systematic process that engages the whole regional community.

---

**Public Information and Warning:** Deliver coordinated, prompt, reliable, and actionable information.

---

**Operational Coordination:** Establish and maintain a unified and coordinated operational structure and process.

---

| Prevention                                                                                                                        | Protection                                                                                                                                                         | Mitigation                                                                                                                                                                       | Response                                                                                                                                        | Recovery                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| To avoid, prevent, or stop a threatened or actual act of terrorism.                                                               | To secure against acts of terrorism and man-made or natural disasters.                                                                                             | To reduce loss of life and property by lessening the impact of disasters.                                                                                                        | To save lives, protect property and the environment, and meet basic human needs after an incident has occurred.                                 | To assist communities affected by an incident to recover effectively.    |
| <ul style="list-style-type: none"><li>• Intelligence and information sharing</li><li>• Screening, search, and detection</li></ul> | <ul style="list-style-type: none"><li>• Access control</li><li>• Physical protective measures</li><li>• Risk management</li><li>• Supply chain integrity</li></ul> | <ul style="list-style-type: none"><li>• Long-term vulnerability reduction</li><li>• Risk and disaster resilience assessment</li><li>• Threat and hazard identification</li></ul> | <ul style="list-style-type: none"><li>• Critical transportation</li><li>• Operational communications</li><li>• Situational Assessment</li></ul> | <ul style="list-style-type: none"><li>• Infrastructure systems</li></ul> |

---

**Cybersecurity:** Establish and maintain a cybersecurity program.

---

**Training and Exercises:** Prepare DOT employees for their roles

---

**Figure 3.** Fundamental and Necessary Capabilities of State DOTs

# Planning

**Conducting a systematic process that engages the whole regional community in the development of executable strategic, operational, and community-based approaches to meet defined objectives that are implementable using available resources and within the time constraints set forth by the agency.**

As a part of their function, state DOTs are responsible for creating all-hazards plans and ensuring that employees have the ability to implement them. These all-hazards plans must conform with and complement the planning activities of the rest of the state's operations and agencies as well as those of regional authorities. DOTs may coordinate planning efforts with other state agencies, including the state's emergency management agency; county highway departments; various agencies of the U.S. DOT; and with DOTs from other states to ensure activities can be easily integrated when necessary. DOTs also need to plan to receive and use resources provided by other states and the federal government during operations. In conducting these planning activities, DOTs should consider applicable standards and best practices for incorporating risk and resilience into asset management functions and system design.

## Key Planning Capabilities

- Use an all-hazards approach.
- Integrate security into planning.
- Ensure consistency with national planning programs.
- Coordinate planning for agency-wide consistency.
- Coordinate with regional partner plans and processes.
- Maintain support and participation from the top (critical).
- Ensure adequate distribution of plans.
- Review and update plans regularly.

The types of plans a DOT may create include:

- Infrastructure protection and security plans
- All-hazards mitigation plans
- Agency-wide emergency operations plan
- A continuity of operations (COOP) plan and COOP site whose capabilities are assessed on a regular basis
- Infrastructure and cybersecurity recovery/resiliency plans
- Communication plans

## Principles to Incorporate Security into Planning

- Risk-based designs
- Redundant components
- Support response
- Facilitate recovery

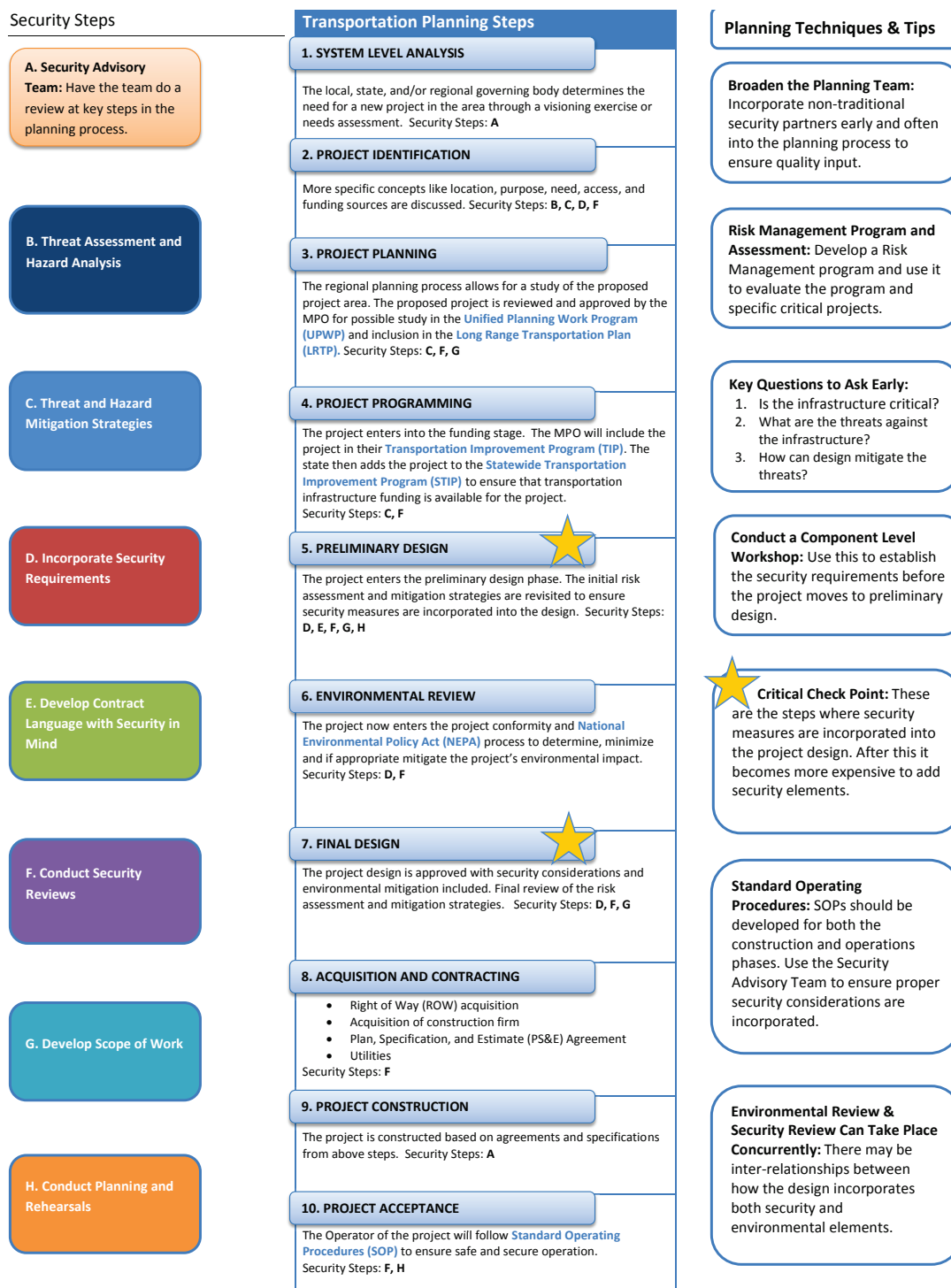


**Figure 4.** Potential linkages to consider security in the project planning process. See the FHWA document to find suggested techniques and tips to help inform planning discussion about infrastructure protection and security.

Source: *Integrating Security into the Project Planning and Development Process*, [http://www.planning.dot.gov/documents/Integrating\\_Security\\_into\\_Project\\_Planning.pdf](http://www.planning.dot.gov/documents/Integrating_Security_into_Project_Planning.pdf)

## Planning Resources

*Considering Security and Emergency Management in the Planning of Transportation Projects: A Guide for Planners of New Transportation Projects* (May 2012)

<http://www.planning.dot.gov/documents/consideringsecurityandem.pdf>

A guide developed by the U.S. Federal Highway Administration to help ensure that security and emergency management are considered during the planning phase of highway-related infrastructure projects. The intended audience is the transportation infrastructure project community, especially transportation planners at a state DOT or a regional metropolitan planning organization (MPO). The guide includes checklists, examples, and resources.

*Integrating Security into the Project Planning and Development Process* (2012)

[http://www.planning.dot.gov/documents/Integrating\\_Security\\_into\\_Project\\_Planning.pdf](http://www.planning.dot.gov/documents/Integrating_Security_into_Project_Planning.pdf)

This brochure outlines linkages for security planning into the project planning process and provides techniques and tips along with resources to help inform discussions about protection and security.

*NCHRP Report 525, Surface Transportation Security, Vol. 16: A Guide to Emergency Response Planning at State Transportation Agencies* (2010).

<http://www.trb.org/main/blurbs/164691.aspx>

This guide provides an overview of high-level requirements for emergency response planning based on national policies, an agency self-assessment, and a resource guide with organization staffing guidance, decision-making sequences, and resource lists.

*TCRP Report 86, Vol. 8/NCHRP REPORT 525, Surface Transportation Security, Volume 8: Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies* (2005)

<http://www.trb.org/main/blurbs/156474.aspx>

The guidelines were designed to assist transportation agencies in operations plans, policies, and procedures consistent with the National Incident Management System. Downloadable worksheets, template for a COOP plan, brochures to explain COOP planning process for staff, a customizable PowerPoint for executive leadership, and 300-plus resources organized in an electronic library are included.

*Generic Continuity of Operations/Continuity of Government Plan for State-Level Transportation Agencies* (2011)

<http://transweb.sjsu.edu/project/1080.html>

This report covers the research conducted to determine how to integrate COOP/COG into the overall NIMS approach to emergency management, including a connection between the emergency operations center (EOC) and the COOP/COG activity.

*NCHRP Research Results Digest 333/TCRP Research Results Digest 90, Natural Hazards Informer Number 4, A Guide to Planning Resources on Transportation and Hazards* (2009)

[http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp\\_rrd\\_333.pdf](http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rrd_333.pdf)

This joint NCHRP and TCRP report highlights a framework for thinking about the stages of a disaster and identifies some of the most current and innovative hazard-related research.



*NIPP Supplemental Tool: Incorporating Resilience into Critical Infrastructure Projects (2013)*

<http://www.dhs.gov/publication/incorporating-resilience-critical-infrastructure-projects>

This DHS document report provides a summary of steps that support infrastructure development decisions and investments that will enhance the resilience of critical infrastructure systems.

# Public Information

**Delivering coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard and, as appropriate, the actions being taken and the assistance being made available.**

Customers require timely and accurate travel information. Given the speed and frequency with which communication travels in today's environment, communicating "regularly and often" may mean multiple times per day, especially during emergencies. As a public entity, the agency may be inundated with requests for public information. Demonstrating a commitment to honest transparency with information and public data can help build and maintain an agency's reputation.

## **Key Public Information Capabilities**

- Make sure that effective communications mechanisms and people are in place so that the agency can communicate regularly and competently to all stakeholders.
- Maintain clear and streamlined communications, with coordination and a cooperative attitude among all process stakeholders.
- Communicate regularly and often.
- Be proactive by releasing relevant and related public data.
- Leverage all appropriate communication means such as social media sites and web-based and mobile technology.
- Provide 24/7 travel information and timely alerts and warnings.
- Coordinate public information and establish procedures to ensure that DOT "speaks with one voice" and releases consistent information to the public and the media.

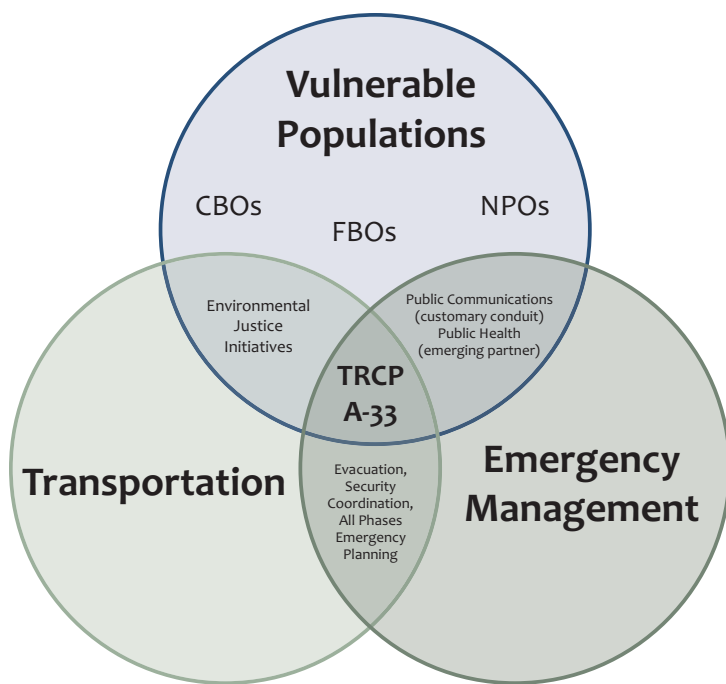
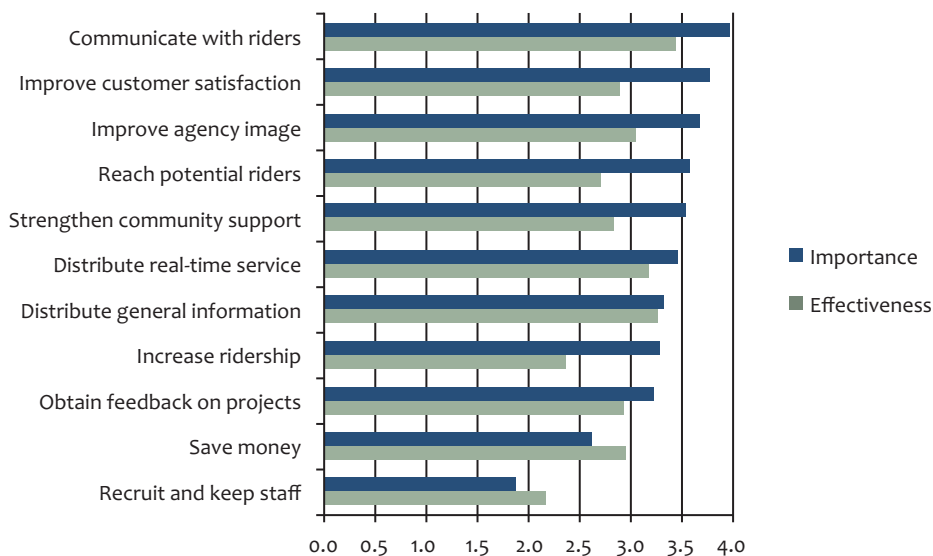


**Figure 5.** Communication Overlap with Transportation, Emergency Management, and Vulnerable Populations.

Source: TCRP Report 150: Communication with Vulnerable Populations: A Transportation and Emergency Management Toolkit (2011)



Compare importance of agency goals and effectiveness of social media in achieving goals. (A weighted average was calculated from responses using four-point scale where “not important/effective at all” = 1 and “very important/effective” = 4. N/A responses were excluded.)

**Figure 6.** Agency Goals vs. Effectiveness of Social Media.

Source: TCRP Synthesis 99: Role of Social Media in Public Transportation (2012)

## Public Information Resources

*TCRP Report 150: Communication with Vulnerable Populations: A Transportation and Emergency Management Toolkit* (2011)

<http://www.trb.org/main/blurbs/166060.aspx>

This guide describes how to create a communication process to reach vulnerable populations regarding their transportation options in emergencies. The toolkit provides a guiding framework and tools for constructing a scalable, adaptable communication process built on a network of agencies from public, private, and nonprofit sectors.

*NCHRP Report 690: A Guidebook for Successful Communication, Cooperation, and Coordination Strategies between Transportation Agencies and Tribal Communities* (2011)

<http://www.trb.org/main/blurbs/165472.aspx>

This guidebook includes guidelines designed to help DOTs and tribal communities work together to achieve successful transportation projects on tribal lands. It offers a flexible approach that can be adapted to most situations and includes case studies to illustrate successful practices.

*TCRP Synthesis 99: Uses of Social Media in Public Transportation* (2012)

<http://www.trb.org/main/blurbs/167067.aspx>

This report explores the use of social media among transit agencies and documents successful practices in the United States and Canada.



# Operational Coordination

**Establishing and maintaining a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.**

DOTs need to understand the specific procedures and protocols that have been established by other local, state, and federal agencies that may become involved with the DOT, especially those for managing incidents and emergencies. DOT staff should stay current regarding the applicable state and national standards for emergency preparedness and response. The federal government expects state DOTs to incorporate principles and concepts of national initiatives that provide common approaches to incident management and response in emergency response plans and operations. National initiatives include the National Response Framework (NRF) with its designated emergency support functions (ESFs) and the National Incident Management System (NIMS) with its protocols for multiagency interaction and communication. State and local NIMS compliance is a prerequisite for federal preparedness funds.

## Key Operational Coordination Capabilities

- Establish internal state transportation agency communications protocols.
- Integrate and synchronize actions of participating organizations and jurisdictions to ensure unity of effort.
- Enhance and maintain NIMS-compliant command, control, and coordination structures to stabilize the incident and transition to recovery.
- Collaborate with all relevant local and regional partners.
- Establish clear lines and modes of communication among partner organizations and jurisdictions.
- Coordinate with appropriate local, regional, and national partners such as non-government organizations.